IN THE SPECIFICATION

Please amend the paragraph on page 1, beginning on line 20, as follows:

File infector viruses typically attach themselves to program files, usually selected .COM or .EXE files although some viruses can infect any executable program. When the program is loaded, the virus is loaded as well. A file infector virus may arrive at a computer as a self-contained program or script sent as an attachment to an e-mail, or via an infected removable storage medium. System or boot-record infector viruses infect executable code found in certain system areas on a disk. They attach to the disk operating system (DOS) boot sector on diskettes or the Master Boot Record on hard disks, and can make the computer's hard disk temporarily unusable. Macro viruses are among the most common viruses, but tend to do the least damage. Macro viruses can infect an application, such as inserting unwanted words or phrases when using a word processing application.

Please amend the paragraph on page 1, beginning on line 33, as follows:

Existing anti virus software scans each file for all known viruses that can affect that type of file. If there are N identical files located on M systems within a local area network (LAN), despite the files being identical, each of these N files is scanned by the anti virus program running on the respective local systems.

Please amend the paragraph on page 2, beginning on line 25, as follows:

It is common for vulnerabilities to viruses to persist within large networks for an unacceptably long time, because removal of the vulnerability requires pro-active steps by many individuals. This exposure can be reduced by managers or the information technology (IT) department within an organisation carefully checking that action has been taken to resolve the vulnerability for all users' systems, but pro-active involvement of managers or IT service teams involves significant costs to the organisation.

Please amend the paragraph on page 7, beginning on line 29, as follows:

In addition, the present specification also discloses a computer readable medium for storing a computer program for performing the operations of the methods. The computer readable medium is taken herein to include any transmission medium for communicating the computer program between a source and a destination. The transmission medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a general purpose computer. The transmission medium may also include a hard-wired medium such as exemplified by typical Internet-connected server computers, or a wireless medium such as exemplified in the global system for mobile communications (GSM) mobile telephone system.

Please amend the paragraph on page 12, beginning on line 12, as follows:

Referring to Figures 4 and 6, a distributed architecture according to one embodiment of the invention comprises a pool server data processing system 60, which includes one or more repositories 400 storing data on behalf of the local server itself and on behalf of the other data processing systems 70 in the local area network 10. In particular, the pool server's repositories 400 store hash values for files stored on each of the data processing systems within the LAN which files have been classified as virus-free. In a simple LAN, such as shown in Figure 1, the pool server system may be a central server 60 or any one of the systems in the LAN which is capable of maintaining the repository 400 and running virus scan coordinator software 100. Of course, a more complex LAN may comprise tens or hundreds of interconnected computer systems and may form part of a wider network (a wide area network (WAN), intranet or the Internet).

Please amend the paragraph on page 27, beginning on line 21, as follows:

One specific solution for making vulnerability and vulnerability resolution information accessible uniformly (from multiple software vendors) is to make the information available as a Web Service using extensible markup language (XML). Additional text information could be provided with a detailed description of a vulnerability, to describe the vulnerability to various users or system administrators.